State of NC
Cloud Computing Strategy

Prepared by:

Agency CIO Cloud Strategy Workgroup

August, 2012

Document History

Version	Date	Author	Comments
1.0	8/16/12	Strategy Workgroup	Initial draft

For more information contact:

State of NC - Office of the State CIO

Enterprise Strategy and Architecture

3900 Wake Forest Rd

Raleigh, NC 27609

Contents

Executive Summary

Background and Approach

In April, 2012, Chief Information Officers from North Carolina Executive Branch agencies sponsored a strategy workgroup to respond to and plan for the increasing demand for cloud computing services. The CIOs recognized that cloud computing could provide significant benefits, but also carried potential risks. Previous cloud computing initiatives within state government had been ad hoc, with little to no formal planning.

The workgroup was asked to develop a formal cloud computing strategy that included, at minimum, the following elements:

- A definition of "cloud computing" generally and within state government in particular
- An analysis of current and future business and technology drivers
- Decision-making guidelines for cloud computing services
- Risk considerations
- Specific recommended next steps

Key Findings

The work group loosely adopted the Federal Government's National Institute of Standards and Technology (NIST) definition, which describes cloud computing as an IT sourcing and delivery model for enabling adaptive, convenient, on-demand network access to a shared pool of configurable computing resources. Common characteristics of cloud computing approaches include on-demand service, broad access, resource pooling, rapid elasticity, and measured services. Cloud-based services can be delivered via on-premises, owned infrastructure (aka a "private cloud"), by subscribing to external services (a "public cloud"), or some combination thereof (a "hybrid cloud").

Cloud services are generally packaged and sold in one of three "flavors":

- SaaS – Software as a Service - Application functionality is rented from a service provider rather than buying, installing and running software yourself. (Fairly common in state government.)

- PaaS – Platform as a Service - Provides a platform in the cloud, upon which applications can be developed and executed. (Not common in state government.)
- IaaS – Infrastucture as a Service - Vendors offer computing power and storage space on demand. (Becoming more prevalent in government environments.)

There are several pertinent market trends in cloud computing. These include a substantial increase in deployments due to increasing numbers of vendor offerings and maturity. Consumers of cloud services are beginning to recognize the importance of interoperability between cloud suppliers, and the need for utmost flexibility and speed from vendors, to fully realize the value proposition. Also, some companies and organizations are exploring off-premises private cloud solutions after fully understanding the cost and complexity of setting up an on-premises service.

In state government, agencies vary greatly in their capability and experience with cloud computing. An informal poll showed an overwhelming majority of agencies are at least evaluating cloud solutions, so this first draft of a formal strategy document comes at an opportune time. Section 3 provides a detailed analysis of the current statewide environment and overall plans for evaluating and migrating to cloud computing solutions.

The work group's primary finding is that state government needs clear, consistent guidelines and decision points for cloud computing services. These guidelines should correlate with a formalized IT investment strategy that maximizes the use of available funds and ensures that business needs are met in the most cost effective manner possible. Section 4 outlines a possible approach to cloud computing in state government.

Key Recommendations

Given the common problems, opportunities, understanding of market trends and current situation, the work group recommends that the following actions be taken immediately:

1. Formalize cloud computing adoption and sourcing guidelines for the enterprise (state). Establish qualifications for cloud computing opportunities.
2. Formalize sourcing management for cloud services.
3. Establish measures for determining the success and value of cloud computing solutions.
4. Identify high value candidate applications/systems and pursue cloud solutions when/where appropriate and/or expedient.

5. As outlined by the 2012 budget bill, prepare a detailed implementation plan for a statewide private cloud by January 2013.[1]

A proposed decision matrix is included for consideration (see Section 4.2). This chart helps illustrate the relationship of various decision factors and the types of computing solutions that agencies should consider.

While the promise of cloud computing is strong, there are serious risks and operational challenges that should be considered, including the following (see Section 4.3 for a detailed explanation):

- *Compliance*
- *Data location*
- *Security*
- *Data recovery*
- *E-discovery*
- *Availability and reliability*
- *Portability and vendor lock-in*

The relative success or failure strategies and directions outlined in this document should be measured in terms of economic outcomes, business alignment, and certain organizational measures. A detailed discussion regarding these measures can be found in Section 4.4.

[1] Section 6A.9, Session Law 2012-142

[2] The complete NIST definition can be found at http://csrc.nist.gov

[3] Gartner Industry Research Note # G00168504; *Cloud Computing in Government: Private, Public, Both or*

Context

1.1 Purpose

In April, 2012, Chief Information Officers from North Carolina's Executive Branch agencies sponsored the formation of a strategy workgroup to respond to and plan for the increasing demand for cloud computing services across the enterprise. The CIOs recognized several important facts:

- Cloud computing may provide efficiencies and cost savings;
- There are also significant risks, both known and unknown;
- The state has not formally considered or planned for cloud computing services to date; recent ventures have been ad hoc;
- Cloud computing stakeholders include not only IT groups, but agency business units, legislators, policy makers, planners, budgets, and more.

The Agency CIO group developed the following deliverables for the workgroup:

- A definition of "cloud computing" within the context of the general IT market and within state government in particular;
- An analysis of current and future business and technology drivers;
- Decision-making guidelines for cloud computing services;
- Risk considerations;
- Specific recommended next steps.

The team that compiled this report and recommendations was comprised of the following executive branch agency representatives:

- Gary Alexander (Office of Information Technology Services)
- Patrick Blalock (Department of Health and Human Services)
- Mike Fenton (Office of the State CIO/Strategy)
- Greg Jones (Department of Public Safety)
- Chip Moore (Office of the State CIO/Enterprise Security and Remediation Management Office)
- Thomas Parrish (Department of Cultural Resources)

- Tim Pursell (Office of State CIO/Architecture)
- Arvind Wathore (Office of State CIO/Architecture)
- Brian Williford (Department of Transportation)

Working part time, the group spent approximately two months researching, discussing and drafting this report. This document is intended to be regularly revisited and updated to reflect changes in technology, business goals, market changes, and other pertinent internal and external drivers.

1.2 Definitions

As a first order of business, the group adopted the Federal Government's National Institute of Standards and Technology (NIST) definition for "cloud computing" as follows:[2]

Cloud computing is an *IT sourcing and delivery* model for enabling adaptive, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It is not a new technology. The cloud model promotes availability and is composed of five essential **characteristics:**

- ***On demand self-service*** – a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

- ***Broad network access*** – capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs).

- ***Resource pooling*** – the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

[2] The complete NIST definition can be found at http://csrc.nist.gov

- ***Rapid elasticity*** – capabilities can be rapidly and elastically provisioned, in some cases automatically. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- ***Measured Service*** – cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled and reported providing transparency for both the provider and consumer of the utilized service.

The state recognizes that cloud services can be delivered via on-premises, owned infrastructure (a "private cloud"), by subscribing to external services from a vendor (a "public cloud"), or leveraging some combination thereof (a "hybrid cloud"). The risks and technical considerations of these various delivery models vary greatly and the recommendations later in this document carefully consider these facts.

Further delineation of cloud computing models also present three important distinctions in the business problems each approach intends to solve:

Software as a Service (SaaS)	Offers renting application functionality from a service provider rather than buying, installing and running software yourself. Examples include Salesforce.com and Gmail.
Platform as a Service (PaaS)	Provides a platform in the cloud, upon which applications can be developed and executed. Examples include Salesforce.com, through Force.com, and Microsoft (Azure).
Infrastructure as a Service (IaaS)	Vendors offer computing power and storage space on demand. Examples include, Rack-space and Amazon S3.

1.3 Business Context

State government is structured as a series of services. These are services to citizens and services internal to state government. The IT Strategic planning process builds upon this business context. Each strategy fits within the framework and results in a manageable, measurable and cohesive set of services. This framework is captured in a separate document called the ***Enterprise Architecture Reference Guide***.

A comprehensive discussion about cloud computing includes not only elements of the technical foundation, but also IT solutions and IT business alignment. As such, the subject matter of this document is considerably broader than other statewide technology strategies.

Of particular note, the NC General Assembly has also recognized the value of cloud computing in recent legislation SB950, prompting the State CIO to develop a detailed plan for the creation of a private cloud to provide IaaS services by January, 2013.

1.4 Industry Trends

A number of industry trends are influencing the cloud computing market. Gartner reports that hundreds of private cloud pilots were deployed in 2011, and that many more pilots and full rollouts will occur in 2012.

Information Technology trends evolve in the marketplace from the initial introduction of the technology, a period of time where "hype" does not align with the expectations of the consumer, followed by a time when there is a disillusionment related to the technology. Finally, the technology matures in the marketplace, is well understood by consumers and can generally be deployed with confidence. Cloud computing, specifically the private cloud, is beginning to enter the last phase of adoption where expectations and capability are in alignment.

The major trends influencing cloud computing are:

1. **Actual deployments** of cloud technology in 2012 will increase the maturity of vendor offerings.
2. **Interoperability** among cloud suppliers is becoming increasingly important.
3. An increasing number of **vendor offerings** are available.
4. As companies and organizations consider adoption, some are searching for external private cloud solutions (**sourcing options**) after realizing the changes necessary to implement a private cloud.
5. **Flexibility** and speed to deploy are increasingly being recognized as key business needs in place of direct cost savings.

Current Cloud Computing Trends

Growing Expertise

As cloud infrastructure expands the number of professionals available to help organizations manage and deploy cloud infrastructure will increase. Best practices and case studies will be published as a result of these deployments and organizations making plans for cloud infrastructure will be able to adopt the lessons learned by the early adopters.

Interoperability and Sourcing Options

IT organizations are becoming the broker to a set of IT services that are hosted internally and externally — *a hybrid computing environment*. Hybrid computing refers to the coordination and combination of external cloud computing services and internal infrastructure. Hybrid computing requires significant integration or coordination between the internal and external environments at the data, process, management or security layers. Most large companies will use some form of hybrid computing. While hybrid computing may not be immediately needed by many organizations, considerations of interoperability and sourcing alternatives should be included in deployment plans. Software that aids in the management of multiple cloud environments is referred to as a cloud broker.

By being the intermediary of IT services, IT organizations can offer internal customers the price, capacity, and speed of provisioning of the external cloud while maintaining the security and governance the company requires and reducing IT service costs.

Vendor Offerings

The number of vendors offering cloud computing services and products continues to be dynamic. Market consolidation has started and will continue in 2012. Virtualization technologies introduced into many organizations do not have services for management of cloud infrastructure. A virtualization vendor does not have to be same entity as the management vendor.

Flexibility

On the whole, the ability to quickly deploy infrastructure in order to meet key business initiatives is becoming more important than direct cost savings. The ability to react to disruption in the market or the individual organization is also growing in importance verses additional savings. Private cloud pilots focused on specific business objectives that are in turn aligned with customer requirements are key factors for early success of cloud adoption.

New Decision Frameworks Developed

As cloud solutions are implemented in an organization, the focus of IT resources can shift to more value-added activities for business and away from lower IT infrastructure support activities. However, these prospective benefits must be examined carefully and mapped against a number of challenges, including security, lack of transparency, concerns about

performance and availability, the potential for vendor lock-in, licensing constraints and integration needs. Over time, cloud computing will not always save money.

These issues create a complex environment in which to evaluate individual cloud offerings. This complexity is further increased by the fact that the requirements and constraints of particular workloads and the datasets associated with them have a significant impact on the potential benefits and risks of various cloud models. Companies will increasingly codify and formalize frameworks to evaluate particular cloud services options based on the characteristics of specific workloads and the security and compliance needs of the associated datasets.

1.5 Current and Emerging Business Needs

As discussed in the business context section, the nature of government's business is diverse. As a result, business needs for government agencies vary widely, sometimes even within an agency. Nonetheless, all agencies have several common business drivers that link directly to information technology solutions. This section outlines some of the common challenges.

Need for Cloud Adoption Guidelines:

Hardly a day goes by without cloud computing coming up in a business meeting. Marketing material from every vendor emphasizes cloud computing in some shape or form. Sometimes, the messaging from vendors is contradictory, creates confusion and raises concerns about cloud computing. Some of these concerns are related to moving states' data to the cloud. Those include ownership and security of data, e-discovery requests and the ability to move the data in house if the vendor goes out of business. In short, there is widespread confusion about cloud services and their advantages and disadvantages.

While some aspects of cloud computing are still evolving, other components have matured and been adopted by organizations.

Given the transformative impact of cloud computing on business, agencies are looking for clear guidelines on how to adopt cloud computing and realize the benefits without putting business at risk. In absence of clear guidelines, agencies may resort to ad-hoc adoption of cloud. This may result in increased risk and increased expenditure to the business. In order to avoid ad-hoc adoption, a reasonable cloud adoption strategy is needed to provide broad guidelines and direction, while still allowing some latitude.

Such a strategy should be based on several factors, including potential business impacts, application suitability for cloud, application risk profile, economic analysis, desired business

agility, business criticality, end-user requirements and statutory needs. With adoption of a cloud service or applications, the role of IT department changes from being a provider of IT infrastructure services to managing a vendor who provides these services. Therefore, the cloud strategy should also give guidance on how to manage a cloud applications, including governance and vendor management. The recommendations section of this document provides a framework for cloud adoption.

Need for Effective Use of Funds:

The current budget climate in North Carolina requires agencies to implement new cost-efficient methods in business process as well as information technology. At the same time, recent technological advancements such as mobility and cloud computing is raising expectations for IT, and citizens are demanding more transparency from their government. Therefore, agency CIOs are looking for ways to optimize IT investments in order to align IT with mission-critical business needs. Infrastructure and people managing the infrastructure make up biggest portion of IT spend. Therefore, it makes sense to focus cost optimization efforts on IT infrastructure.

Ability to Address Emerging Business Needs:

As outlined in the Industry Trends section, flexibility to quickly deploy infrastructure and address market disruptions are two major trends impacting how IT investment decisions are made. Mobility is one of the technologies causing market disruption and changing the way business services applications are developed and consumed. Employees invest their own money to buy latest technology and mobile devices, and expect to be connected to the enterprise network anywhere at any time. A recent study conducted by CISCO states that the number of wireless devices will more than triple by the year 2020.

Businesses want IT to provide applications that work with new mobile devices and support these applications, without increasing costs. They also want these services to be rapidly deployed and scaled up or down based on the demand. On-premise cloud solution is one way to provide this flexibility. An on-premise cloud solution requires an infrastructure backbone that can be provisioned and orchestrated with ease. It requires a flat network with one unified way of provisioning and managing all resources, such as computing, network, and storage. In a cloud-ready network, various layers of infrastructure are converged to reduce maintenance tasks, devices and overall complexity. State agencies see a demand for converged infrastructure in order to not only support new usage and consumption pattern but to lower IT infrastructure management cost.

Present State of Cloud Computing

2.1 Government – General

Migrating to cloud based services usually involves a detailed evaluation of the readiness of applications and data and the business case. The challenges in the government sector are no different from that of the private sector, but issues surrounding procurement and security are more pronounced for government.

Budgeting for government is much different than the private sector. Government IT budgets are planned well in advance, often a few years before, leaving agencies with little flexibility for last-minute changes. The selection of vendors and service providers is a long and involved process designed to procure services at the best value for the state. Because of the nature of the process, government may find it more difficult to procure IT services from niche service providers that can deliver innovative services at low prices. Therefore, government and their agencies are working to change the traditional procurement models as they become serious about procuring IT resources via the cloud. The following chart provides a basic framework government and their agencies are seeking as they migrate to cloud base services:

Reduction in IT Spending	By adopting cloud computing, agencies can create a central pool of shared resources – software and infrastructure. The consolidation of resources and the could reduce IT spending.
Agility	Governments operate in a strict hierarchical manner and the process for approvals and purchase orders is a time consuming activity. Cloud computing provides the capability to eliminate these time consuming activities and provision resources on the fly.
Access to Most Updated Technology	Cloud computing offers government the ability to constantly access to the most updated software and hardware. The onus of upgrading technology is on the service provider in this delivery model, not the state.
Elimination of Procurement & Maintenance	Cloud computing could eliminate the need to procure, monitor and maintain common IT resources. Apart from reducing the workload, this reduces the need for IT staff and allows government and agencies to focus on their core areas.
	Cloud computing is delivered through the Internet, enabling universal access to

Universal Resource Access	resources. Furthermore, it helps the government in establishing a common platform that is easily accessible for all its eGovenment initiatives.

Security and Return on Investment are the key factors as governments evaluate and pilot cloud base services. Service providers are responding to these requirements by creating dedicated government clouds to meet those demands.

Service providers are also adding additional layers of security through a variety of means including bio-metric scanners, locked racks, separate caging for government servers and remote security verification services. Increasingly, providers are looking at third-party security audits and certifications such as SAS 70 and ISO 27001 to validate their claims and to lessen concerns.

To offer more value, service providers are provisioning government clouds in community cloud models dedicated for government customers. This allows government departments and agencies to leverage a shared resource pool and drive cost efficiencies. Furthermore, the network infrastructure is dedicated to offer more stringent Service Level Agreements and guarantees to meet the high availability requirements of government agencies.

2.2 "Ownership" vs. "Control" of Government Cloud Services

Consolidation of IT services is a long-running theme in both the public and private sectors. This is commonly referred to as "shared" or "centralized" IT services. Shared services are primarily focused on creating economies of scale, increasing standardization and mitigating risks. With the rapid evolution and availability of cloud computing services for IT infrastructure and application services, government organizations need to seriously consider the advantages, disadvantages, risks, and costs associated with this new sourcing option for IT services.

Within cloud computing, it is important to recognize the differences between the "ownership" of cloud computing services and the "control" aspects of the data and functionality. Gartner defines this difference as follows :

***Ownership** concerns the provider of cloud services that are used by government agencies. The owner can be either a single government organization, or a cluster of government*

organizations sharing resources, or a third party. Regardless of ownership, government organizations need to exercise different levels of <u>control</u> on how those services are delivered. Some of this may be granted by the programmatic interface of those services, but some areas like data location, security, availability and e-discovery, where control is needed for regulatory compliance purposes, may require peculiar contractual constraints.[3]

Gartner provides further elaboration on the cloud services ownership/sourcing perspective by defining six categories of government cloud computing service models[4] that could exist depending on who has access to cloud services and who owns those services as follows :

- ***Internal single agency :*** Resources used to deliver the services are owned by a single agency and are used for its exclusive benefits. From an infrastructure perspective, this is equivalent to virtualizing significant computing resources of an agency and making them accessible as a service providing the attributes of scalability and elasticity that are typical of the cloud. In general, single-agency cloud services will support mission-critical workloads in large and very large agencies where infrastructure utilization is already very efficient, the existing infrastructure meets the scalability and elasticity needs of current and prospective workloads, and low latency is required. For instance, the IT organization of a tax and revenue agency may establish an internal cloud platform to provide infrastructure or application services to different divisions within that agency.

- ***Shared single agency :*** Resources are scattered across multiple government organizations but are virtualized in such a way to provide a per-use service to a single government organization. These are adequate for large agencies' workloads where higher latency is tolerable (such as periodic batch applications). There are two different cases, both relatively rare: (1) where previously independent agencies are merged together; and (2) where a government IT organization serves different agencies and manages resources that physically reside in those agencies and uses part of these to provide cloud services to a large agency. In most cases, though, shared cloud services will be of a multiagency nature — i.e., used by several agencies.

- ***External single agency :*** In this case, a large agency accesses cloud computing services from a third party (i.e., an IT service vendor). For infrastructure services offerings, this is close to an IT infrastructure utility model, which is an enterprise-class offering by a

[3] Gartner Industry Research Note # G00168504; *Cloud Computing in Government: Private, Public, Both or None?*; Andrea Di Maio – June 30, 2009
[4] Gartner Industry Research Note # G00168504; *Cloud Computing in Government: Private, Public, Both or None?*; Andrea Di Maio – June 30, 2009

provider that allows government clients to access infrastructure services on the provider's terms. Alternatively, this could result from a full outsourcing model.

- ***Centralized multiagency :*** A large agency or a newly established government organization provides cloud services that can be used by multiple agencies or by selected nongovernment organizations or both. The service is centralized so that there is no participation by users in the governance of the cloud computing services. An example would be a whole-of-government IT service provider that already provides a variety of infrastructure and application services to several agencies and decides to adopt the characteristics of cloud computing services to improve utilization and reduce costs.

- ***Shared multiagency :*** This is a true shared-service arrangement, where a cluster of government organizations (ranging from a few to all those in a jurisdiction) share the governance of the cloud computing services they access. Many existing shared-service organizations may morph into cloud computing service providers where cloud computing characteristics help deliver better services and the scale of use justifies such a model. The membership in a multiagency cloud can extend beyond government organizations in a given jurisdiction on a selective basis.

- ***External multiagency :*** Several agencies use cloud computing services provided by an external provider. This can be the evolution of a shared multitenant cloud, an external single-tenant one, or a third-party offering that provides services to a bounded set of clients. In the first case, government resources used for a shared model are transferred to an external service provider; in the second case, an external service provider offers utility arrangements to a cluster of agencies that can procure those collectively or through a framework contract; in the third case, a cluster of agencies joins a service that is already provided by an external service provider for limited membership.

Using the above definitions, Appendix B contains a summarization of current cloud service initiatives and SaaS solutions being utilized within the State of North Carolina. This appendix was constructed using the documents and associated information that was self-reported by State agencies in support of the ***Applications Hosted Outside of State Infrastructure Report*** that was delivered by the SCIO to the General Assembly in October 2011.

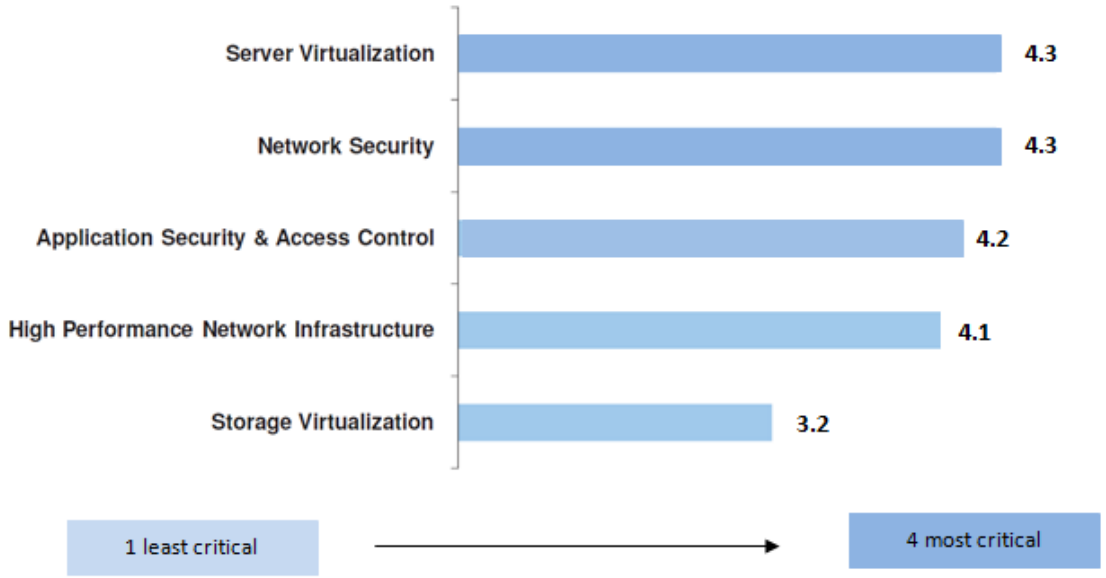
2.3 State of North Carolina

Components in Building a Cloud

From a purely technical perspective, cloud computing represents a carefully orchestrated synthesis of many enabling infrastructure technologies. This includes a broad array of

computing, storage, and communications capabilities, as well as associated management systems and tools.

In developing a comprehensive cloud strategy, it is essential to first understand the current state and different components that are essential to build and maintain a cloud that meets government requirements. According to a recent Gartner study, governments have allocated highest priority to server virtualization and network security. This is consistent with North Carolina's priorities. Server virtualization will help governments meet their resource consolidation objectives. Furthermore, security is paramount to government adoption. Governments will adopt cloud computing only if they are convinced that their data will remain secure and available. The following chart illustrates the priority attached to different components in building a cloud based on data collected from North Carolina agencies currently adopting cloud or cloud-like services.



Note: Data for the above chart derives from agency business leader survey and current strategic initiatives.

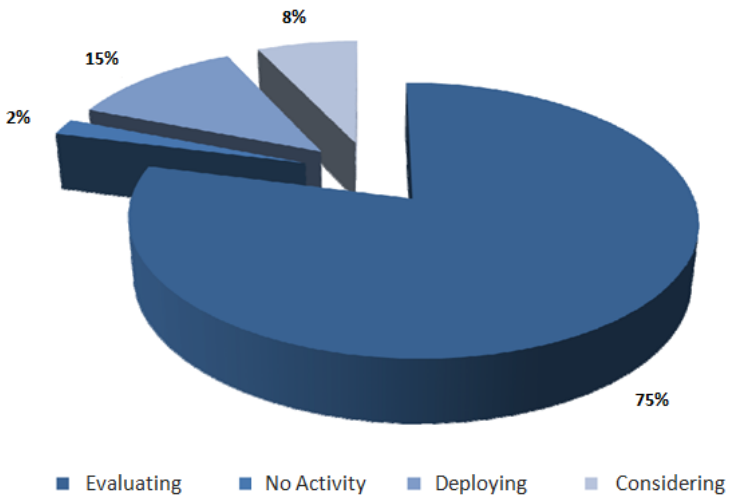
State in Executive Government Adoption Trends

Executive agencies are looking at cloud services to bring efficiencies to their IT landscapes. They are looking to enhance their own IT infrastructure and reduce IT spending. They also believe that by establishing a cloud computing ecosystem, they will be able to provide better services.

Data collected by the workgroup suggests that 98 percent of the executive branch agencies are deploying, evaluating or considering cloud computing in one form or the other. Furthermore, the data revealed that given the State's concerns around security of data and

location of data centers, private and hybrid clouds are witnessing significantly higher adoption or consideration.

Cloud Computing Adoption Percentage among Executive Branch Agencies



Finding the Right Balance

Adoption of cloud computing is growing in government, but concerns over reliability, security and privacy, data governance, data retention, and protection of intellectual property is slowing the pace.

In order to overcome these issues, policy makers must strike the right regulatory balance in ensuring flexibility, regulatory compliance and jurisdiction.

2.4 General Conclusions/Observations for Cloud Computing in Government

The workgroup reached the following general conclusions about cloud computing in the public sector:

- Cloud solutions are becoming a viable sourcing option for IT services but government is not moving aggressively to transition mission-critical IT services into off-premise cloud services.

- Cloud computing for government has a number of risks associated with it including issues relating to security, data privacy, portability, access, and vendor lock-in.
- In its simplest form, public or private cloud computing is nothing more than another sourcing option for government organizations that need a more scalable, flexible, and virtualized IT infrastructure or application services.
- Cloud computing services being used by government entities can be sourced and managed by government organizations, external providers, or some combination of the two.
- Cloud computing services for government are no different than any other kind of shared government service in that success or failure will be determined in part by the appropriate and efficient governance for the shared service as opposed to the technical adequacy of the solution.
- Cloud computing services should be approached as an alternative sourcing opportunity for IT services and it should be evaluated based upon the benefits, costs and risks.

Future State and Recommendations

3.1 Future Cloud Computing Environment

As the state analyzes, plans, designs, and architects cloud computing solutions, critical success factors must be considered:

Governance

Because shared cloud services pose challenges similar to other kinds of shared government services, success or failure will depend on the shared-service governance more than on the technical aspects of the solutions. Decisions concerning service levels, changes, investments, sourcing strategies and pricing must be subject to discussion and approval by a formalized management structure that is uniquely qualified to determine if and how cloud computing services are best leveraged within the larger information technology environment.

As with any shared service, it is important that all cloud services, both private and public, are properly bounded by applicable technical and architectural standards. It is also critical for the state to establish and maintain associated technology roadmaps for a planning horizon of no less than two years.

Resources

While cloud services generally reduce the need for ongoing capital investments and flatten O&M spending, it is still important to properly plan for necessary financial and human resources. This includes new and enhanced roles such as strategic sourcing, contract negotiation, vendor management, and service level management.

Supporting Policies, Processes and Systems

The decision to implement and utilize cloud services is primarily of a sourcing and service management nature. As such, the state must ensure that ancillary systems and supporting policies and processes are appropriately retrofitted to facilitate adoption, reduce risks, improve efficiencies, and ensure viability. This includes:

- *Procurement processes* that include special terms and conditions to reduce risks that are unique to cloud computing environments (see Risk section later in this document).
- *Chargeback systems* that accommodate consumption-based billing
- *Security policies* that properly balance the risks and efficiencies that cloud computing solutions introduce
- *Integration capabilities* to improve the ability to monitor, report, and manage cloud computing solutions as seamless extensions to traditional infrastructure services.

Cloud computing decisions must also be couched within the overall strategic IT planning context of the state. This includes an impact analysis of related projects, technical capabilities, program goals, cost constraints, architectural considerations, etc.

Many IT groups will need to reevaluate current organizational structures in order to effectively and efficiently manage cloud computing solutions. On-premises private cloud services, for example, introduce a level of technology convergence that will invalidate most "silo"-based approaches to managing IT infrastructure. On the other hand, off-premises public cloud services shift operational focus from purely tactical activities to longer term service management roles. IT organizations will need to adjust accordingly.

3.2 Recommendations

Recognizing the inevitability of cloud computing, business units within the state must be prepared to make carefully measured business and sourcing decisions in response to certain problems and opportunities. Moreover, IT organizations need to proactively develop technical capabilities to fully leverage the benefits that cloud computing can facilitate.

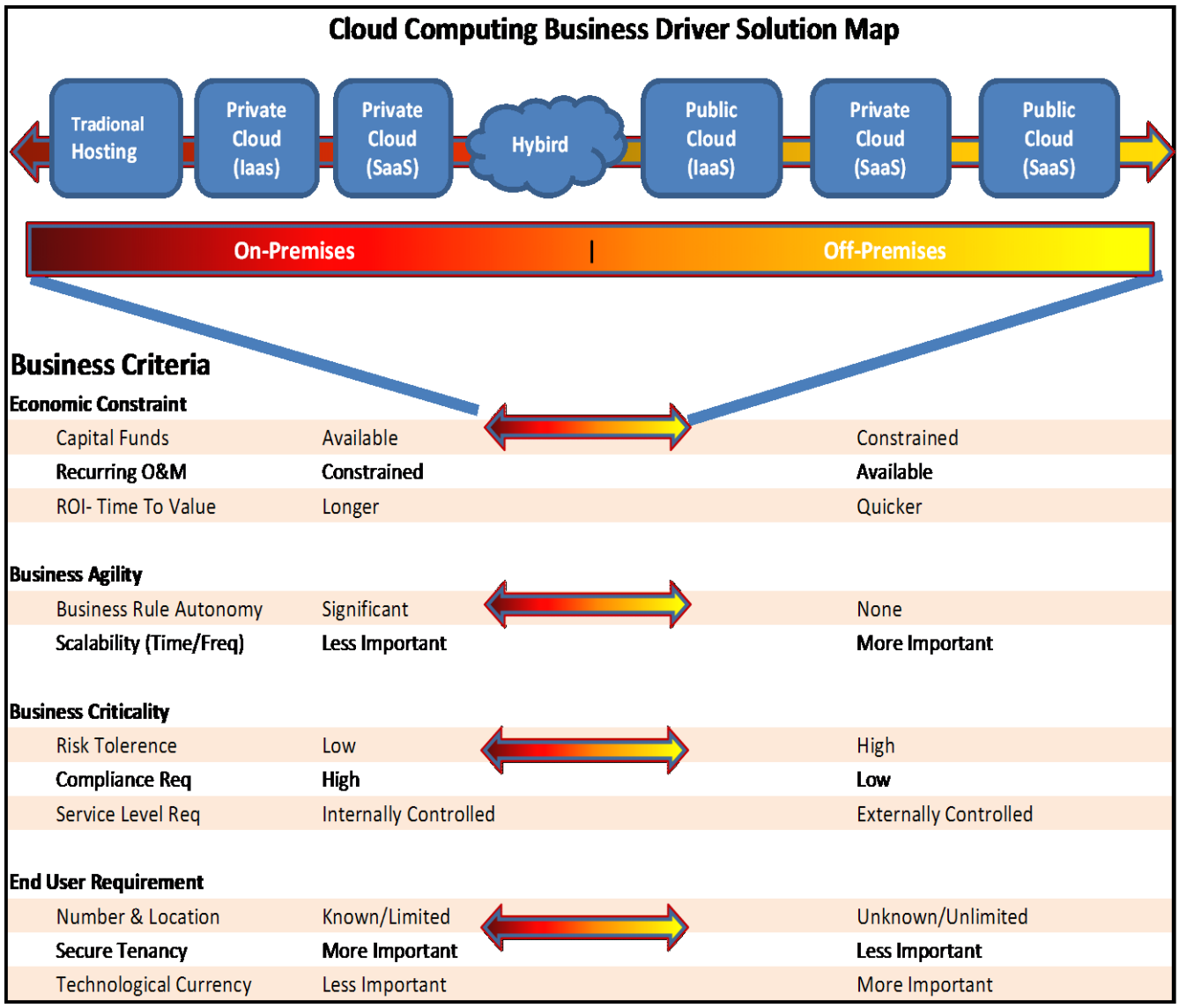
Considering the common problems and challenges, industry trends, and emerging agency business requirements, the workgroup recommends the following actions:

1. Formalize cloud computing adoption and sourcing guidelines for the enterprise (state). Establish qualifications for cloud computing opportunities.
2. Formalize sourcing management for cloud services.
3. Establish measures for determining the success and value of cloud computing solutions.
4. Identify high value candidate applications/systems and pursue cloud solutions when/where appropriate and/or expedient.
5. As outlined by SB950, prepare a detailed implementation plan for a statewide private cloud by January 2013.

An Approach to Cloud Computing

4.1 Deciding and Sourcing Cloud Services

While there are literally thousands of possible technical permutations, the major categorizes of distributed computing solutions and the essential business drivers can be illustrated as follows:



Business Criteria			
Economic Constraint			
Capital Funds	Available		Constrained
Recurring O&M	**Constrained**		**Available**
ROI- Time To Value	Longer		Quicker
Business Agility			
Business Rule Autonomy	Significant		None
Scalability (Time/Freq)	**Less Important**		**More Important**
Business Criticality			
Risk Tolerence	Low		High
Compliance Req	**High**		**Low**
Service Level Req	Internally Controlled		Externally Controlled
End User Requirement			
Number & Location	Known/Limited		Unknown/Unlimited
Secure Tenancy	**More Important**		**Less Important**
Technological Currency	Less Important		More Important

This chart helps illustrate the relationship of various decision factors and the types of computing solutions that agencies should consider. Six major categories of computing solutions are presented on a continuum ranging from traditional on-premises hosting to public off-premises cloud services. A "hybrid" solution appears in the middle of the continuum simply to illustrate the potential for actual solutions to combine elements of the other solution sets. Four key decision categories are outlined, with more granular considerations for each.

Those involved in making a hosting decision for an IT application or system can use this chart to help constrain choices and focus on those with the most value. As each of the business criteria is considered, the result will correlate on a relative basis to the continuum of computing solutions, suggesting better or worse fits for each particular criterion. This diagram makes no assumptions regarding weighting for any of the individual criteria, so the

decision maker will need to apply individual judgment in determining how the totality of the measures should be considered.

Definitions

Economic Constraints	Identify any funding constraints that exist. Off-premises cloud solutions can help an agency work around limited capital investment funding, but typically require steady, ongoing O&M commitments. Cloud computing solutions also help drive a quicker return on investment, but internal investments often yield larger returns.
Business Agility	Identify the need for the business to be agile. This includes two different views. First, the business must determine to what degree it needs to remain in control of business rules, how frequently they change, and how unique they are. Second, the need for scalability needs considered. Agencies that are extremely unique, must be in full control of business rules, and are relatively static are probably not candidates for cloud computing solutions at this time. On the other hand, cloud solutions fit well in environments where the business can make sure of "commodity" solutions in which the business rules are understood and standardized across an industry. Agencies with seasonal activities should also consider cloud-based solutions due to the ease and cost effectiveness by which the number of consumers can shrink and grow on demand.
Business Criticality	Determine the risk tolerance profile for the business. Agencies with significant compliance requirements, no risk tolerance, and a need to control service level expectations may want to limit solutions to on-premises approaches.
End User Requirements	Assess the needs of the consumers of the service in question. Cloud solutions are typically most cost effective for large populations of diverse users. Cloud providers also tend to have a strong commitment to refreshing underlying technology and keeping solutions technically aligned with the market. However, by definition, cloud computing solutions make extensive use of shared resources and as such are more difficult to separate into secure tenancies.

4.2 Risks

Challenges and Risks of Cloud Computing in Government

As with any technology deployment, security must be a critical element in any discussion of cloud computing. Cloud services must be governed and managed with the same or higher rigor than existing state IT services. Regardless of the cloud model in question, there are

certain risks that must be identified and considered in developing a cloud computing strategy.

- ***Compliance :*** Statutory requirements are as applicable to cloud services as they are to any other approach for managing state government information assets. Depending on the data being hosted, an organization must be able to demonstrate a provider's compliance to any number of standards or statutory requirements, such as FISMA, IRS 1075, PCI DSS, and HIPAA. It is also important to consider that some federally protected data may not be able to be placed in a cloud environment without a written agreement from the actual owner of the data. This agreement will need to be in place prior to movement into the cloud. The degree to which cloud providers will accept liability in their service agreements, for exposure of content under their control, may be insufficient. In addition to industry standards and statutory requirements, cloud computing services must be evaluated against statewide security standards and statewide architectural requirements. Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.
- ***Data location :*** To ensure low cost and scalability, cloud-based services do not generally provide any assurance about where client data is being hosted on the provider's network. The cloud's premise is that data exists within the Internet's global infrastructure. Some cloud providers maintain large data centers in multiple locations and they prefer not to specify publicly their exact locations, often for their own security and continuity of operations protection. With an increasingly globalized infrastructure, this implies that clients cannot know for certain which country their data is located. This may pose challenges to comply with data protection regulations. Further, some countries that share a common privacy regulatory framework (such as in the EU) may have national regulations similar to the USA Patriot Act that allow the relevant authorities to seize data hosted on any server located in their jurisdiction for national security purposes.
- ***Security :*** There are typical data movement security issues and data storage security issues. Cloud offerings may use Secure Sockets Layer (SSL) to protect data while in transit; however, a majority of cloud offerings store data in shared environments. Data and information classification is critical for cloud-computing arrangements. Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Sensitive or confidential data that is processed beyond the government's control or by nongovernmental employees or contractors can increase the level of risk and liabilities not only for the government organization but also for its citizens. As a result, cloud providers will have to demonstrate, and perhaps constantly certify, their security capabilities (for example, disaster recovery, intrusion protection

and access controls). For instance, an agency or government could require that all public data being stored and backed up in the cloud be encrypted thus trying to limit who has access to decryption keys. In addition, organizations must consider issues with identity management, access controls, user account and service monitoring, and vulnerability management processes.

- ***Data recovery :*** Organizations need to ensure that data is replicated so that it can be recovered from cascading critical incidents or natural and man-made disasters. A question to ask is, "Do cloud-based services provide assurance that data and applications are replicated across multiple sites to reduce vulnerability?" Also, “How quickly can data be recovered when needed?”
- ***E-discovery :*** Internal investigations of illegal or inappropriate activity, as well as legal or administrative electronic discovery requests, are time-intensive and time-consuming endeavors, even when conducted on a government-owned infrastructure. The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. Also, such services are difficult to audit, because data and access logs for multiple clients are co-located and are likely to be spread across an ever-changing set of hosts and data centers.
- ***Availability and reliability :*** Vendors claim that availability and reliability are major advantages of the cloud, and it is designed to be flexible and scalable to meet multiple demands. It is not yet the case that the service-level agreements (SLAs) they offer would meet the requirements of all government specific, mission-critical processes. While it is not uniquely related to cloud-based services, it is not clear what would happen if cloud-based services were discontinued or how users would access their data if they lost their Internet connections. Related to this issue is a provider’s cyber security incident response plan. How would a provider respond to a cyber-security incident and would it be sufficient to meet an organization’s requirements?
- ***Portability and vendor lock-in :*** There are issues regarding an organization's ability to easily retrieve its data (and business processes performed in embedded software services) should it decide to terminate services with a cloud provider (or if the provider goes out of business or suffers from supply-chain disruptions from other providers). Also of concern is how to securely remove data from a provider’s storage when the cloud computing service is terminated. What assurance is there that all instances of an organization’s data have been securely removed? The commingling of one customers’ data with other customers’ data complicates this issue. While these risks also exist when data and applications are sourced internally, the cloud exacerbates them, because it may be extremely difficult to copy huge amounts of data or securely remove huge amounts of data from a cloud provider across the Internet, particularly if there is no existing mechanism for it.

4.3 Measurements

Success of the cloud computing strategy is based on enterprise wide adoption of cloud decision framework and further execution of successful cloud computing projects. In order to determine success of cloud computing projects, proper measures must be defined. One of the most commonly used measures to justify investment in technology is return on investment (ROI). ROI focuses on the cost and associated benefits in financial terms. It provides limited or no visibility into actual business benefits or value realization. Without business benefits, it is difficult to justify any investment. Therefore, cloud computing measures must establish a direct linkage between benefits derived and business outcomes. These measures must also address the challenges and opportunities discussed in earlier sections.

Because this is a strategy document and not a detailed implementation roadmap, this section describes broad guidelines on what metrics should be established, how measurements should be done within the context of business outcomes, and finally how measures should be communicated to the business. The metrics discussed below are just an example and are not meant to be comprehensive list of all possible metrics. Thus, agencies have freedom to design their own metrics specific to their situation and articulate the impact on business outcomes. For sake of discussion, the metrics are divided into three broad categories.

Economic Measures

a. Capital Expenditure Avoidance
b. Optimized Operational Expenditure
c. Transparency of IT cost

Business Alignment Measures

a. Service Availability
b. Business Agility
c. Aligned with emerging business needs

Organizational Measures

a. Adoption of cloud decision framework

Economic Measures

The immediate and well known benefit of cloud computing is the reduction in cost. By using cloud computing services, business can avoid capital expenditure. In addition IT operational

cost are reduced because virtualized environments use less data center resources such as physical space, power and cooling. Cloud based services often provide usage based billing. These measures by themselves are not meaningful to the business, unless they are discussed within the business context. IT organizations should use these measures as a means to improve transparency of IT spend and communicate effective use of IT dollars to address business needs.

Business Alignment Measures

The economic measures discussed above communicate to the business that IT is using the limited funds wisely. However, the real value of cloud computing is in measuring how IT services are aligned with the business and how IT spend is helping business transformation. IT needs to measure intangible metrics to communicate these non-financial benefits to the business. Some of these measures include benefits of cloud computing such as business agility, service availability and elasticity.

In IT terms, Gartner defines agility as - how quickly an IT service, capacity allocation scheme, workload distribution plan, etc., can adapt to changing demand situations and business environments, or technology scenarios, with varying performance and service levels, in near real time[5]. For example, if IT can reduce time to provision new service or application by two months, what is the business benefit? In those two months, if business can process 10,000 more licenses renewal applications, then there is visible benefit to the business. Linking IT service agility to the actual business benefits makes it easier for business to understand the value of IT.

Other measures such as service availability and elasticity should also be tracked and linked to tangible business benefits. For example, service availability (reduced down time) and elasticity (ability to handle unexpected peaks in demand) can result in business benefits such as decrease in help desk calls by 20% and increased customer/citizen satisfaction.

Disaster Recovery (DR) is inherently built into cloud services. As more and more services adopt cloud infrastructure, businesses reduce their risk and gain ability to recover in case of disaster. The business value from DR can be, the number of business process that are covered by DR and ultimately support Business Continuity.

Similarly cloud services have built in ability to be accessible from anywhere and via any device. The business outcome of this ability is to address new business opportunities via

[5] Gartner Industry Research Note # G00218589; Business-Aligned Metrics for IT Services in Cloud: Returns on Agility, Elasticity, Continuity and Consistency; Tapati Bandopadhyay,10 January 2012

mobile platforms. The benefit to the business is new channels of communication with the citizens.

Organizational Measures

The Recommendation section of this document explains how to use various decision factors to decide what types of computing solutions are best suited for a business process. Adoption of this decision framework should enable agencies in making informed decision about suitability of cloud computing for a business specific need. One measure of successful adoption is less confusion and reduction in the number of queries from agencies regarding when cloud computing makes business sense and when it does not.

In summary, these measures try to focus on value rather than cost, and on business outcome rather than IT output. The idea is to connect IT services to their realized value or benefit in supporting business outcomes. And finally, the ultimate goal of the business should be to strike a balance between various measures for successful cloud strategy adoption and execution.

Appendix A

State IT Design Principles

(Summarized from the February, 2011 State IT Plan)

Simplification	Simplification addresses time and expenses related to managing complexity. Planning should include re-examining existing practices and simplifying them when needed.
Consolidation	Consolidation seeks ways to reduce or eliminate duplication. Planning should consider aggregation, resource pooling, and virtualization as appropriate.
Customer Segmentation	Segmentation is grouping customer populations according to similar demands or constraints. IT solutions should be designed and architected to cost-effectively meet the unique needs of each segment.
Application Delivery	Application delivery comprises the mechanisms and methods for providing business functionality to customers through the use of technology tools and systems. Application delivery should cost-effectively meet customer business needs while ensuring required applications are available when needed, protect customer information and data as required and provide convenient methods for customer access.
Mobility	Mobility recognizes the increasing need for application and data availability from geographically diverse locations. Applications and business data must be deliverable anywhere and at any time to meet customer requirements.
Technology Roadmaps	A technology roadmap is a plan matching short and long term business goals with specific technology solutions to help meet those goals. Technology roadmaps should be created and maintained to maximize overall return on technology investment, leverage economies of scale, avoid obsolescence, and prepare for the future.

Appendix B

Cloud Services Inventory

(Summarized from a 2011 report to NC State Legislature)

The following inventory was produced using the (6) primary categories of government cloud computing services as defined by Gartner. The individual inventory items were acquired from the ITS Service Catalog as well as from the documents that were self-reported by State agencies in support of the "Applications Hosted Outside of State Infrastructure Report" that was delivered by the SCIO to the GA in October 2011. A best effort was made to map all of these Iaas/SaaS services into the (6) different categories although we think it is safe to assume that some of these mappings may not be 100% accurate given the limited information that is currently available for some of these (external) services being used by various agencies. In some cases, the service being utilized would be more consistent with Data-as-a-Service (DaaS) as opposed to IaaS or SaaS. It is also important to note that there may be other applications within any given agency that could/would qualify for one of the "single agency" categories but insufficient information is available at this time to make this determination.

Internal Single Agency – IaaS/SaaS Services

- None reported

Shared Single Agency – IaaS/SaaS Services

- None reported

External Single Agency – IaaS/SaaS Services

- DOT – Constructware (provided by AutoDesk)
- DOT – NCETS emissions (provided by Verizon)
- DHHS – NC Info and Referral (provided by North Light, Inc.)
- DPI – Teach/Principal Eval Tool (provided by McRel, Inc.)
- DPS – Offender Tracking and Electronic Monitoring (provided by G4S)
- DPS – Offender Mgmt Mapping Tool (provided by MapQuest)
- DPS – Adult Offender Supervision (provided by ICOTS)
- DPI – Learning Management Services (provided by Blackboard)
- DPI – e-Linguafolio English as a second language (provided by MCNC)
- DPI – CTE Conference Registration Application (provided by Design Hammer)
- DPI – CE Conference Registration Application (provided by Design Hammer)

- DPI – Common Core and Standards Transitions (provided by Wikispaces)
- DPI – Collaborative Web Sites for Divisions (provided by Intrafinity)
- DPI – Sharp School Collaboration Tool (provided by Sharp School)
- NCCCS – Learning Management Services (provided by Blackboard)
- NCCCS – eMail Archiving (provided by MS Computer Generated Solutions)
- NCCCS – eMail services (provided by MS Live @ EDU)
- NCCCS – Small Business Center (provided by Center Dynamics)
- NCCCS – Video Conferencing (provided by Microsoft via Skype)
- COM – CRM Application (provided by SalesForce.com)
- COM – WorkforcePlus Client Tracking Application (provided by Sumtotal)
- COM – Grants Management (provided by CyberGrants)
- COM – Accountable Results for Community Action (provided by Community Action Opportunities)
- WRC – BigGame IVR Application (provided by Angel.com)
- WRC – Hunter & Boater Education (provided by Kalkomey Enterprises)
- DST – File Transfer Services (provided by Leapfile)
- DOL – Jurisdiction Online (provided by Praeses)

Centralized Multiagency – IaaS/SaaS Services

- Common Payment Services (provided by ITS/OSC)
- BEACON (provided by OSC)
- NCID (provided by ITS)
- Directory Services (provided by ITS)
- Intrusion Protection Services (provided by ITS)
- Firewall & VPN Services (provided by ITS)
- Remote Access VPN Services (provided buy ITS)
- Mainframe Hosting (provided by ITS)
- Distributed Hosting (provided by ITS)
- Data Base Hosting (provided by ITS)
- WAN Network Services (provided by ITS)
- LAN Network Services (provided by ITS)
- WLAN Services (provided by ITS)
- Managed Desktop Services (provided by ITS)
- Structured Cabling Services (provided by ITS)

Shared Multiagency – IaaS/SaaS Services

- eMail Messaging, eMail Archiving, and Calendar Services (provided by ITS)
- Video Conferencing (provided by ITS)

- Telephony Services (provided by ITS)
- Contact Center Services (provided by ITS)
- Yahoo Stores eCommerce Web Sites (provided by Yahoo via ITS)
- IT Service Management (provided by ITS)
- Software Quality Assurance (provided by ITS)
- Electronic Content Management Services
    - Electronic Document Management (provided by ITS)
    - Document Scanning (provided by ITS)
    - Document UI/Portal (provided by ITS)

External Multiagency – IaaS/SaaS Services

- Innotas Project & Portfolio Management Services (SaaS solution used by ITS)
- Web Conferencing (provided by Carahsoft Technology Corp. via ITS)
- Managed Print Services (provided by Systel and KM Data via ITS)
- OSP – Enterprise eRecruit System (provided by NeoGov)
- OSP – NC Flex Web Enrollment (provided by Aon Hewitt)
- OSC – Learning Management System for BEACON Training (provided by Noverant)
- DOA – WITS Mail Tracking (provided by The Alternative)

References

In addition to specific references through this document, the following additional sources were also utilized:

Gartner: Five Cloud Computing Trends

Gartner: Top Five Trends for Private Cloud Computing

Gartner: Predicts 2012: Cloud Computing Becoming a Reality

Gartner: 2012 Cloud Computing Planning Guide: From Hybrid IT to Hybrid Clouds

Federal Cloud Computing Strategy

http://www.cloudave.com/15290/PaaS-is-the-future-of-cloud-services-heroku-adds-scala-and-cumulogic-goes-openstack/

http://cloudtimes.org/2011/06/22/cloud-computing-its-current-market-trends-and-future-opportunities/

http://gigaom.com/cloud/how-todays-cloud-services-foretell-a-post-aas-world/

http://cloudninja.codeplex.com/

http://bits.blogs.nytimes.com/2011/04/21/amazon-cloud-failure-takes-down-web-sites/

http://montclairadvisors.com/blog/2011/12/saas-predictions-for-2012/

End of document